Halte aux hackers

4e édition

Stuart McClure
Joel Scambray
George Kurtz

© Groupe Eyrolles, 2003, pour la présente édition,
ISBN : 2-7464-0486-9

OEM
EYROLLES

Table des matières

Préface XXIII
Avant-propos XXV
L'ignorance, voilà l'ennemi (bis) XXV
Quoi de neuf dans la quatrième édition ? XXVI
Conventions utilisées dans cet ouvrage XXVII
Mode d'emploi d'un piratage réussi XXVIII

PARTIE I

Connaissance de l'organisation 1
Étude de cas : surveillance de la sécurité du réseau 1
Réponse aux incidents mettant en œuvre la surveillance de la sécurité du réseau 7

CHAPITRE 1
Prise d'empreinte 9
Qu'est-ce que la prise d'empreinte ? 9
Prise d'empreinte Internet 11
Étape 1 – Déterminer le champ d'activités 11
Étape 2 – Recensement des éléments de réseau 16
Étape 3 – Interrogation d'un serveur DNS 25
Étape 4 – Reconnaissance du réseau 30

CHAPITRE 2
Balayage 35
Déterminer si le système est actif 35

Recherche des services actifs ou en écoute 43
Types de balayage 44
Identification des services TCP et UDP actifs 46
Outils Windows de balayage de ports 52
Répartition des types de balayage de ports 57
Détection du système d'exploitation 60
Prise d'empreinte active de pile 61
Prise d'empreinte passive de pile 65
La panoplie complète : les outils d'exploration automatisés 68

CHAPITRE 3
Recensement 71
Capture élémentaire de bannières 72
En résumé… 125

PARTIE II

Piratage de systèmes 127
Étude de cas : les risques des tests d'intrusion 127

CHAPITRE 4
Piratage de Windows 95/98/Me 131
Attaques à distance de Windows 9*x* 133
Connexion directe à des ressources partagées de Windows 9*x* 133
Portes dérobées et chevaux de Troie pour Windows 9*x* 139
Vulnérabilités répertoriées des applications serveur 144
Attaques locales contre Windows 9*x* 145
Windows Millennium Edition (Me) 151
Attaques à distance de Windows Me 152
Attaques locales contre Windows Me 152
En résumé… 154

CHAPITRE 5
Pirater la famille Windows NT 155
Attaques sans authentification 157
Attaques SMB (Server Message Block) 158
Attaques IIS 176

Attaques avec authentification 185
Élévation des droits 186
Chapardage 191
Contrôle à distance et portes dérobées 201
Redirection de port 206
Parades générales aux attaques avec authentification 207
Masquer ses traces 212
Fonctions de sécurité des systèmes NT 214
Installation systématique des derniers correctifs 215
Stratégie de groupe 215
IPSec 217
Commande runas 218
.NET Framework 219
Pare-feu de connexion Internet 220
Système de fichiers chiffrés 220
Une note sur les raw sockets et autres critiques sans fondement 221
En résumé… 222

CHAPITRE 6
Pirater Novell NetWare 225
Liens aux serveurs Novell 226
Recenser la bindery et les arborescences 228
Ouvrir les portes non verrouillées 235
Recensement avec authentification 237
Obtention des droits d'accès Administrateur 241
Vulnérabilités des applications 245
Attaques par mystification (outil Pandora) 251
Actions possibles après obtention du statut Admin sur le serveur . . . 254
Accéder aux fichiers NDS 256
Modification des fichiers journaux 262
Fichiers journaux de la console 264
En résumé… 267

CHAPITRE 7
Pirater UNIX 269
La quête du root 269
Bref rappel 270

Cartographie des vulnérabilités 270
Accès distant contre accès local 271
Accès à distance 272
Attaques camouflées dans les données 275
Le shell, le shell, vous dis-je ! 285
Types courants d'attaques à distance 289
Accès local 316
Une fois devenu root 332
Rootkits 332
Récupération après une attaque par rootkit 345
En résumé… 346

PARTIE III

Pirater un réseau 349
Étude de cas : traverser un pare-feu via un tunnel 349

CHAPITRE 8
Pirater un réseau commuté, un PABX, une boîte vocale et un réseau privé virtuel 351
Préparer les attaques téléphoniques 352
Composition automatique de numéros 354
Matériel 354
Considérations juridiques 356
Coûts annexes 356
Logiciels 357
Scripts de force brute : la méthode maison 373
Pirater les PABX 386
Pirater une messagerie vocale 391
Pirater un réseau privé virtuel 396
En résumé… 401

CHAPITRE 9
Équipements réseau 403
Explorer le réseau 404
Détection 404

Interrogations IP 407
Recherche de systèmes autonomes 407
Traceroute classique 408
Traceroute avec ASN 408
show ip bgp 409
Groupes de discussion publics 410
Détection de services 411
Vulnérabilité du réseau 417
Couche 1 du modèle OSI 418
Couche 2 du modèle OSI 419
Détection de supports de couche 2 420
Écoute d'un environnement commuté 420
Couche 3 du modèle OSI 429
Dsniff 431
Mauvaises configurations 434
Piratage du protocole de routage 440
En résumé… 451

CHAPITRE 10

Pirater des réseaux sans fil 453
Prise d'empreinte sans fil 454
Matériel 455
Balayage et recensement des réseaux sans fil 470
Analyseurs pour réseaux sans fil 470
Outils de surveillance de réseau sans fil 473
Contrôle d'accès MAC 481
Obtention d'accès (piratage de 802.11) 483
Contrôle d'accès MAC 484
Attaques contre l'algorithme WEP 486
Sécuriser WEP 488
Outils exploitant les faiblesses de WEP 488
Attaques par déni de service 492
Aperçu de 802.1x 492
En résumé… 494

CHAPITRE 11
Pare-feu 495
Panorama des pare-feu 495
Identification d'un pare-feu 496
Détection de pare-feu avancée 501
Balayages au delà des pare-feu 505
Filtres de paquets 509
Vulnérabilités des proxy applicatifs 512
Vulnérabilités WinGate 514
En résumé… 517

CHAPITRE 12
Déni de service (DoS) 519
Motivations des assaillants 520
Types d'attaques par déni de service 520
Utilisation de la bande passante 521
Épuisement des ressources 522
Défauts de programmation 522
Attaques par routage et DNS 523
Attaques génériques par déni de service 523
Sites attaqués 526
Déni de service pour UNIX et Windows 530
Attaques par déni de service à distance 531
Attaques par déni de service distribué 535
Attaques par déni de service locales 541
En résumé… 542

PARTIE IV

Piratage de logiciels 545
Étude de cas : l'éternel retour 545

CHAPITRE 13
Vulnérabilités du contrôle à distance 547
Détection de logiciels de contrôle à distance 547
Connexion 549

Vulnérabilités 549
Virtual Network Computing (VNC) 557
Microsoft Terminal Server et Citrix ICA 561
Le serveur 561
Le client 562
La transmission de données 562
Trouver des cibles 562
Attaquer Terminal Server 565
Autres considérations sur la sécurité 569
Ressources 570

CHAPITRE 14
Techniques avancées 573
Vol de session 573
Portes dérobées 576
Chevaux de Troie 600
Cryptologie 603
Catégories d'attaques 603
Attaques SSH 604
Violation de l'intégrité système : rootkits et outils miroir 606
Social engineering 609
En résumé… 611

CHAPITRE 15
Pirater le Web 613
Piratage des serveurs Web 613
Divulgation du code source 614
Attaques sur la mise en forme canonique 616
Vulnérabilités WebDAV 617
Dépassements de tampon 620
Vulnérabilités ColdFusion 629
Scanners de vulnérabilités des serveurs Web 632
Piratage des applications Web 633
Trouver des applications Web vulnérables avec Google 634
Exploration systématique du Web 635
Évaluation d'une application Web 637
Vulnérabilités courantes des applications Web 643

En résumé… 649

CHAPITRE 16

Pirater l'internaute 651

Code mobile malveillant 652

ActiveX de Microsoft 653
Failles de sécurité dans Java 663
Attention aux cookies 668
Vulnérabilités des cadres HTML dans Internet Explorer 673

Fraude SSL 675

Piratage du courrier électronique 678

Bases du piratage du courrier électronique 678
Exécuter du code arbitraire via du courrier électronique 681
Vers du carnet d'adresses Outlook 695
Attaques par pièces jointes 698
Enregistrer les pièces jointes sur disque sans intervention de l'utilisateur . 702
Provoquer des connexions sortantes chez le client 707

Pirater IRC 710

Parades globales au piratage de l'internaute 711

En résumé… 713

PARTIE V

Annexes 715

ANNEXE A

Ports les plus courants 717

ANNEXE B

Les 14 principales vulnérabilités 723

Index 725